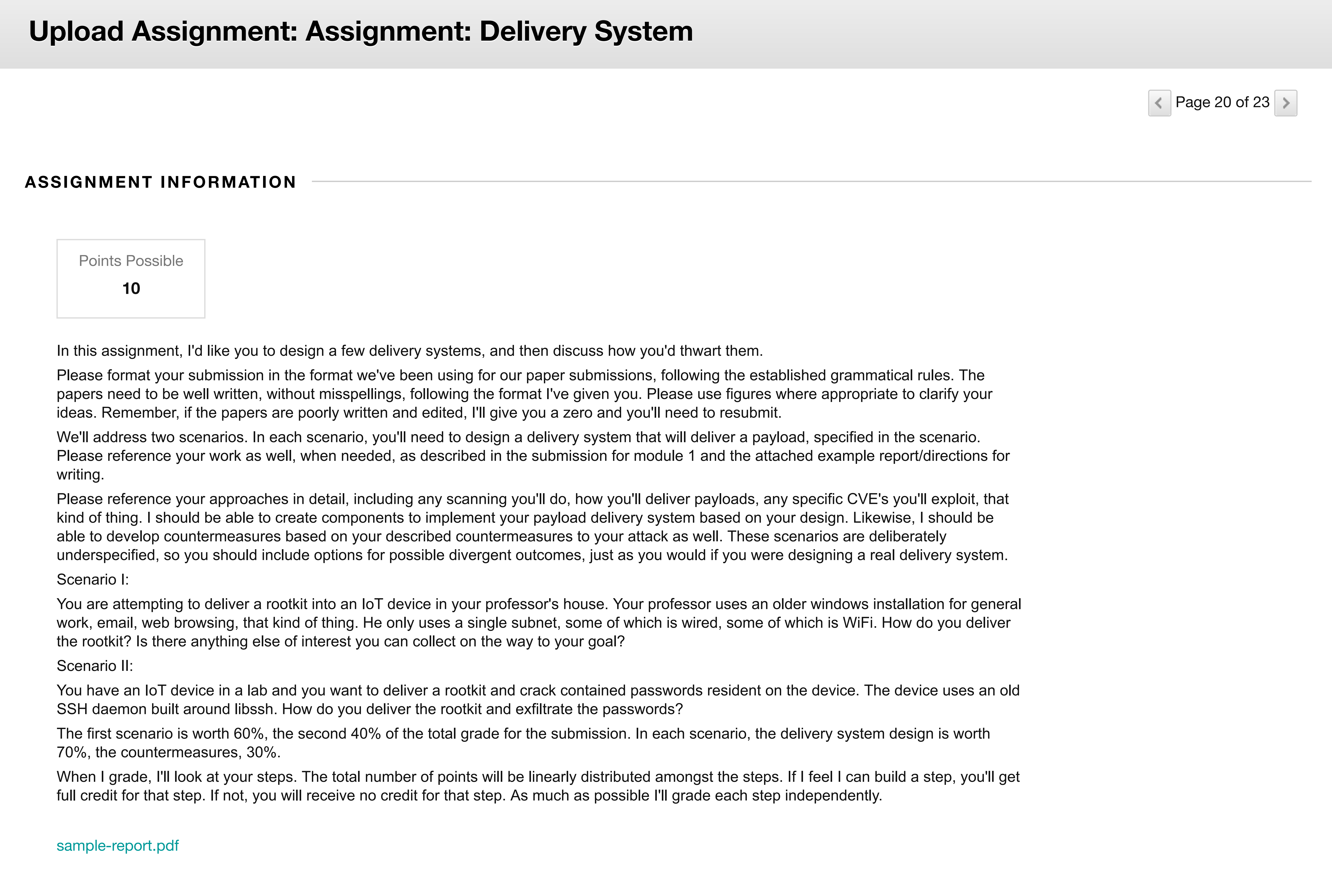

Upload Assignment: Assignment: Delivery System

‹ Page 20 of 23 ›

ASSIGNMENT INFORMATION

Points Possible

10

In this assignment, I'd like you to design a few delivery systems, and then discuss how you'd thwart them.

Please format your submission in the format we've been using for our paper submissions, following the established grammatical rules. The papers need to be well written, without misspellings, following the format I've given you. Please use figures where appropriate to clarify your ideas. Remember, if the papers are poorly written and edited, I'll give you a zero and you'll need to resubmit.

We'll address two scenarios. In each scenario, you'll need to design a delivery system that will deliver a payload, specified in the scenario. Please reference your work as well, when needed, as described in the submission for module 1 and the attached example report/directions for writing.

Please reference your approaches in detail, including any scanning you'll do, how you'll deliver payloads, any specific CVE's you'll exploit, that kind of thing. I should be able to create components to implement your payload delivery system based on your design. Likewise, I should be able to develop countermeasures based on your described countermeasures to your attack as well. These scenarios are deliberately underspecified, so you should include options for possible divergent outcomes, just as you would if you were designing a real delivery system.

Scenario I:

You are attempting to deliver a rootkit into an IoT device in your professor's house. Your professor uses an older windows installation for general work, email, web browsing, that kind of thing. He only uses a single subnet, some of which is wired, some of which is WiFi. How do you deliver the rootkit? Is there anything else of interest you can collect on the way to your goal?

Scenario II:

You have an IoT device in a lab and you want to deliver a rootkit and crack contained passwords resident on the device. The device uses an old SSH daemon built around libssh. How do you deliver the rootkit and exfiltrate the passwords?

The first scenario is worth 60%, the second 40% of the total grade for the submission. In each scenario, the delivery system design is worth 70%, the countermeasures, 30%.

When I grade, I'll look at your steps. The total number of points will be linearly distributed amongst the steps. If I feel I can build a step, you'll get full credit for that step. If not, you will receive no credit for that step. As much as possible I'll grade each step independently.

sample-report.pdf